EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	41	713/150-194.ccls. and template and encrypt$ and decrypt$ and @pd>="20061206"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/23 09:44

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	110	template and (reencrypt$ (re adj encrypt$)) and (public adj key) and certificate	US-PGPUB	OR	ON	2007/03/23 11:14

Published before September 2001
Terms used **template encrypt decrypt**

Found **35** of **124,314**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 35 Result page: **1** 2 next

Relevance scale

1 A fuzzy commitment scheme

Ari Juels, Martin Wattenberg
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press

Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

2 Customization of object request brokers by application specific policies

Bo Nørregard Jørgensen, Eddy Truyen, Frank Matthijs, Wouter Joosen
April 2000 **IFIP/ACM International Conference on Distributed systems platforms Middleware '00**
Publisher: Springer-Verlag New York, Inc.

Full text available: pdf(160.32 KB) Additional Information: full citation, abstract, references, citings

This paper presents an architectural framework for customizing Object Request Broker (ORB) implementations to application-specific preferences for various non-functional requirements. ORB implementations are built by reusing a domain-specific component-based architecture that offers support for one or more non-functional requirements. The domain-specific architecture provides the mechanism that allows the ORB to reconfigure its own implementation at run-time on the basis of application-specif ...

3 Verifying security protocols with Brutus

E. M. Clarke, S. Jha, W. Marrero
October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 4
Publisher: ACM Press

Full text available: pdf(347.12 KB) Additional Information: full citation, abstract, references, citings, index terms

Due to the rapid growth of the "Internet" and the "World Wide Web" security has become

a very important concern in the design and implementation of software systems. Since security has become an important issue, the number of protocols in this domain has become very large. These protocols are very diverse in nature. If a software architect wants to deploy some of these protocols in a system, they have to be sure that the protocol has the right properties as dictated ...

Keywords: authentication and secure payment protocols, formal methods, model-checking

4 Smart Cards and Biometrics: The cool way to make secure transactions
David Corcoran, David Sims, Bob Hillhouse
March 1999 **Linux Journal**
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.95 KB) Additional Information: full citation, index terms

5 Making tuple spaces safe for heterogeneous distributed systems
Naftaly H. Minsky, Yaron M. Minsky, Victoria Ungureanu
March 2000 **Proceedings of the 2000 ACM symposium on Applied computing - Volume 1 SAC '00**
Publisher: ACM Press
Full text available: pdf(777.83 KB) Additional Information: full citation, references, citings, index terms

6 Focus on Software
David A. Bandel
January 2001 **Linux Journal**
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(6.81 KB) Additional Information: full citation, index terms

7 An architecture for a secure service discovery service
Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, Anthony D. Joseph, Randy H. Katz
August 1999 **Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking MobiCom '99**
Publisher: ACM Press
Full text available: pdf(1.47 MB) Additional Information: full citation, references, citings, index terms

8 A probabilistic poly-time framework for protocol analysis
P. Lincoln, J. Mitchell, M. Mitchell, A. Scedrov
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press
Full text available: pdf(1.31 MB) Additional Information: full citation, references, citings, index terms

9 MorphoSys: case study of a reconfigurable computing system targeting multimedia applications
Hartej Singh, Guangming Lu, Eliseu Filho, Rafael Maestre, Ming-Hau Lee, Fadi Kurdahi, Nader

Bagherzadeh
June 2000 **Proceedings of the 37th conference on Design automation DAC '00**
Publisher: ACM Press

Full text available: pdf(968.27 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we present a case study for the design, programming and usage of a reconfigurable system-on-chip, MorphoSys, which is targeted at computation-intensive applications. This 2-million transistor design combines a reconfigurable array of cells with a RISC processor core and a high bandwidth memory interface. The system architecture, software tools including a scheduler for reconfigurable systems, and performance analysis (with impressive speedups) for target applications are desc ...

Keywords: MPEG-2, SIMD, automatic target recognition, dynamic configuration, reconfigurable processors, scheduling

10 Commercial key recovery

Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, David M. Balenson
March 1996 **Communications of the ACM**, Volume 39 Issue 3
Publisher: ACM Press

Full text available: pdf(536.19 KB) Additional Information: full citation, references, citings, index terms, review

11 Technical reports

SIGACT News Staff
January 1980 **ACM SIGACT News**, Volume 12 Issue 1
Publisher: ACM Press
Full text available: pdf(5.28 MB) Additional Information: full citation

12 Superposing Connectors

Michel Wermelinger, Antónia Lopes, José Luiz Fiadeiro
November 2000 **Proceedings of the 10th International Workshop on Software Specification and Design IWSSD '00**
Publisher: IEEE Computer Society
Full text available: pdf(200.08 KB) Publisher Site Additional Information: full citation, abstract, citings

The ability to construct architectural connectors in a systematic and controlled way has been argued to promote reuse and incremental development, e.g., as a way of superposing, à la Carte, services like security over a given communication protocol. Towards this goal, we present a notion of high-order connector, i.e., a connector that takes connectors as parameters, for superposing coordination mechanisms over the interactions that are handled by the connectors that are passed as actual argument ...

13 Secure and mobile networking

Vipul Gupta, Gabriel Montenegro
December 1998 **Mobile Networks and Applications**, Volume 3 Issue 4
Publisher: Kluwer Academic Publishers

Full text available: pdf(223.39 KB) Additional Information: full citation, abstract, references, citings, index terms

The IETF Mobile IP protocol is a significant step towards enabling nomadic Internet users.

It allows a mobile node to maintain and use the same IP address even as it changes its point of attachment to the Internet. Mobility implies higher security risks than static operation. Portable devices may be stolen or their traffic may, at times, pass through links with questionable security characteristics. Most commercial organizations use some combination of source-filtering routers, sophisticate ...

14 Subquadratic zero-knowledge

Joan Boyar, Gilles Brassard, René Peralta
November 1995 **Journal of the ACM (JACM)**, Volume 42 Issue 6
Publisher: ACM Press
Full text available: pdf(1.91 MB) Additional Information: full citation, references, citings, index terms

Keywords: bit commitment, circuit evaluation, communication complexity, cryptography, interactive proofs, matrix multiplication, non-averaging sets, randomness, zero knowledge

15 The UNIX time-sharing system

Dennis M. Ritchie, Ken Thompson
January 1983 **Communications of the ACM**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(658.06 KB) Additional Information: full citation, abstract, references, citings

UNIX is a general-purpose, multi-user, interactive operating system for the Digital Equipment Corporation PDP-11/40 and 11/45 computers. It offers a number of features seldom found even in a larger operating systems, including: (1) a hierarchical file system incorporating demountable volumes; (2) compatible file, device, and inter-process I/O; (3) the ability to initiate asynchronous processes; (4) system command language selectable on a per-user basis; and (5) over 100 subsystems including ...

Keywords: PDP-11, command language, file system, operating system, time-sharing

16 Extending cryptographic logics of belief to key agreement protocols

Paul van Oorschot
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

The authentication logic of Burrows, Abadi and Needham (BAN) provided an important step towards rigourous analysis of authentication protocols, and has motivated several subsequent refinements. We propose extensions to BAN-like logics which facilitate, for the first time, examination of public-key based authenticated key establishment protocols in which both parties contribute to the derived key (i.e. key agreement protocols). Attention is focussed on six distinct generic goals for authenti ...

17 Toward a model of self-administering data

ByungHoon Kang, Robert Wilensky0
January 2001 **Proceedings of the 1st ACM/IEEE-CS joint conference on Digital libraries JCDL '01**
Publisher: ACM Press
Full text available: pdf(308.08 KB) Additional Information: full citation, abstract, references, index terms

We describe a model of self-administering data. In this model, a declarative description of how a data object should behave is attached to the object, either by a user or by a data input device. A widespread infrastructure of self-administering data handlers is presumed to exist; these handlers are responsible for carrying out the specifications attached to the data. Typically, the specifications express how and to whom the data should be transferred, how it should be incorporated when it i ...

Keywords: asynchonous collaboration, data access model, data management, distributed file system, file sharing, peer to peer, scalable update propagation, self-administering data

18 The battle over the institutional ecosystem in the digital environment

Yochai Benkler
February 2001 **Communications of the ACM**, Volume 44 Issue 2
Publisher: ACM Press
Full text available: pdf(93.52 KB) html(34.35 KB) Additional Information: full citation, citings, index terms, review

19 TIPSTER architecture: TIPSTER text phase II architecture concept

Architecture Committee
May 1996 **Proceedings of a workshop on held at Vienna, Virginia: May 6-8, 1996**
Publisher: Association for Computational Linguistics
Full text available: pdf(1.28 MB) Additional Information: full citation, abstract

The TIPSTER Architecture is a software architecture for providing Document Detection (i.e. Information Retrieval and Message Routing) and Information Extraction functions to text handling applications. The high level architecture is described in an Architecture Design Document. In May 1996, when the initial architecture design is complete, an Interface Control Document will be provided specifying the form and content of all inputs and outputs to the TIPSTER modules.

20 Secure data hiding in wavelet compressed fingerprint images

Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle
November 2000 **Proceedings of the 2000 ACM workshops on Multimedia MULTIMEDIA '00**
Publisher: ACM Press
Full text available: pdf(688.05 KB) Additional Information: full citation, abstract, references, citings, index terms

With the rapid growth of the Internet, electronic commerce revenue now amounts to several billion US dollars. To avoid fraud and misuse, buyers and sellers desire more secure methods of authentication than today's userid and password combinations. Automated biometrics technology in general, and fingerprints in particular, provide an accurate and reliable authentication method. However, fingerprint-based authentication requires accessing fingerprint images scanned remotely at the user's workst ...

Keywords: WSQ compression, authentication, biometrics, data hiding, fingerprints, watermarking